IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF NEW MEXICO

UNITED STATES OF AMERICA,

Plaintiff,

vs. No. 1:07-cr-386 MCA

LORETTA OTERO,

Defendants.

MEMORANDUM OPINION AND ORDER

THIS MATTER comes before the Court on *Defendant's Motion to Suppress Evidence Seized from Her Computer and Computer Disks* [Doc. 23] filed December 11, 2007. The Court held a hearing on the motion on January 22, 2008. Having considered the parties' submissions, the relevant law, the arguments of counsel and otherwise being fully informed in the premises, the Court grants the motion.

I. FINDINGS OF FACT

The Court enters the following findings of fact:

1. Defendant was a contract mail carrier hired by the United States Postal Service to deliver mail on Postal Highway Contract Route (HCR) 064, and had been the contractor on HCR 064 for approximately thirteen (13) years prior to 2002. [Doc. 28-2, pp. 7–8.]

2. In February 2001, the United States Postal Inspection Service began receiving

complaints and reports of credit card fraud occurring in Los Lunas, New Mexico**.** [Doc. 28-2, pp. 7–8.]

3. The complaints were from victims living on HCR 064. [Doc. 28-2, p. 7.]

4. Stephanie Herman has been a United States Postal Inspector since March 1998. [Transcript of morning proceedings ("Tr.-a.m.") 14:16.]

5. Inspector Herman was assigned to investigate the complaints of credit card fraud along HCR 064. [Tr.-a.m. 14:21–23.]

6. Inspector Herman concluded that the suspect was someone who had direct and consistent access to the mail on HCR 064. [Doc. 28-2, p. 8.]

7. Inspector Herman's investigation led her to suspect that Defendant was intercepting items such as credit cards, credit card applications, credit card statements, affidavits of forgery, and other credit card-related items from the victims' mail. [Doc. 28-2, pp. 8–10.]

8. Inspector Herman came to believe through her investigation that Defendant was using the intercepted mail to fraudulently obtain credit cards in victims' names and then using the fraudulently obtained credit cards to withdraw cash from ATMs. [Doc. 28-2, pp. 8–10.]

9. On March 14, 2002, Inspector Herman arranged for two (2) "test" letters addressed from credit card companies to be delivered to reported credit card fraud victims on Defendant's route. The day the "test" letters should have been delivered to the postal customers, Defendant did not deliver them. After

Defendant had completed her route that day, Inspector Herman intercepted Defendant as she was returning to her personal vehicle. The two "test" letters were found in Defendant's canvas bag along with some of her personal items, one piece of standard mail, and eight pieces of First Class Mail. [Doc. 28-2, pp. 8–9.]

10. On March 14, 2002, Defendant was suspended from her route pending the outcome of further investigation, and advised that she was prohibited from delivering mail. [Doc. 28-2, p. 9.]

11. On March 19, 2002, Inspector Herman sent a letter to all postal customers on HCR 064 asking that they contact her if they had been a victim of credit card fraud within the last two (2) years.

12. Inspector Herman prepared an application and affidavit for a search warrant to search Defendant's residence and to seize Defendant's computer and other computer-related items such as storage media. [Doc. 28-2, pp. 6–12.]

13. In her affidavit, Inspector Herman stated that beginning in February 2001 through March 2002, complaints of credit card fraud were received from approximately sixteen addresses on Defendant's route. [Doc. 28-2, p. 8.]

14. Through her investigation prior to applying for the search warrant, Inspector Herman had obtained the names and addresses of some of the suspected victims of credit card fraud, but the names and addresses were not included in her affidavit. [Tr.-a.m. 45:10–22.]

15. Inspector Herman believed that Defendant likely would be keeping records of victim names, addresses, credit card numbers, and personal identification numbers, and that such records might be found on Defendant's home computer. [Doc. 28-2, p. 10; Tr.-a.m. 18:1–9.]

16. Before Inspector Herman presented the application and affidavit to the United States Magistrate Judge, she submitted the documents to the United States Attorney's office for review and obtained its approval. [Tr.-a.m. 15:5–7.]

17. Inspector Herman's affidavit in support of the search warrant described the investigation and the facts that she asserted provided probable cause to believe that Defendant was the culprit behind the credit card fraud that was victimizing residents on HCR 064. [Doc. 28-2, pp. 6–12.]

18. In the affidavit, Inspector Herman also expressed her belief based on experience that perpetrators of credit card fraud will often keep records of their criminal activity on computer hard drives and disks. [Doc. 28-2, p 10.]

19. She also expressed her belief based on experience that searching for items on computer systems is a highly technical process that must be performed by a qualified computer expert in a laboratory or controlled environment. [Doc. 28-2, p 11.]

20. Information that could have more particularly described the items to be searched for on the computer was available, but omitted from both the warrant and the affidavit presented to the Magistrate Judge.

21. On March 27, 2002, Inspector Herman obtained a search warrant, signed by a United States Magistrate Judge, authorizing the U.S. Postal Inspector to search Defendant's residence for certain items, and to seize all computer-related items. [Doc. 28-2, pp. 1-5; Govt's Ex. 1.]

22. The affidavit in support of the search warrant did not include the names and addresses of any suspected victims nor the names and addresses of all postal customers on HCR 064, nor was such information provided to the Magistrate Judge that issued the warrant. [Doc. 28-2, pp. 6–12; Tr.-a.m. 45:23–25, 46:1–2.]

23. The search warrant incorporated by reference an "Attachment A" describing the premises to be searched, which was Defendant's residence, any structures and outbuildings, and certain vehicles. [Doc. 28-2, pp.1–2.]

24. The search warrant incorporated by reference an "Attachment B" which described the objects of the search. [Doc. 28-2, pp.1, 4,5.]

25. Attachment B is a two-page document consisting of a total of nine numbered paragraphs divided under two headings: "Items to be Seized" and "Computer Items to be Seized." [Doc. 28-2, pp. 4–5.] Attachment B states in its entirety:

ITEMS TO BE SEIZED:

1. Any and all mail matter addressed to residents of Highway Contract Route 064 in Los Lunas, New Mexico.

2. Any and all credit cards, credit card receipts and/or other records bearing names, addresses and/or credit card numbers of known victims

and other residents from Highway Contract Route 064 in Los Lunas, New Mexico

3. Any and all credit cards, credit card invoices, receipts, statements, affidavits of forger, pre-approved offers, applications, correspondence, automatic teller machine (ATM) receipts and/or other records related to credit card or other accounts at financial institutions and/or businesses for individuals other than residents of 123 La Ladera Rd., Los Lunas, NM 87031.

4. Any and all mail matter or correspondence addressed to individuals other than residents of 123 La Ladera Rd., Los Lunas, NM 87031.

5. Any and all materials, including but not limited to letters, correspondence, journals, records, notes, data and computer logs bearing victim information and/or other information related to or pertaining to the theft of mail, the fraudulent credit cards, bank fraud and conspiracy including but not limited to credit card offers, receipts, credit card statements, financial statements, and financial transaction records.

COMPUTER ITEMS TO BE SEIZED

6. Any and all information and/or data stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer or with the aid of computer-related equipment. This media included floppy diskettes, fixed hard disks, removable hard disk cartridges, tapes, laser disks, video cassettes and other media which is capable of storing magnetic coding, as well as punch cards, and/or paper tapes and all printouts of stored data.

7. Any and all electronic devices which are capable of analyzing, creating, displaying, converting or transmitting electronic or magnetic computer impulses or data. These devices include computers, computer components, computer peripherals, word processing equipment, modems, monitors, cables, printers, plotters, encryption circuit boards, optical scanners, external hard drives, external tape backup drives and other computer-related electronic devices.

8. Any and all instructions or programs stored in the form of magnetic or electronic media which are capable of being interpreted by a computer

or related components. The items to be seized include operating systems, application software, utility programs, compilers, interpreters and other programs or software used to communicate with computer hardware or peripherals either directly or indirectly via telephone lines, radio or other means of transmission.

9. Any and all written or printed material which provides instructions or examples concerning the operation of the computer systems, computer software and/or any related device, and sign-on passwords, encryption codes or other information needed to access the computer system and/or software programs.

26. Inspector Herman's affidavit was attached to the warrant. [Tr.-a.m. 22:1–4.]

27. The search warrant did not incorporate by reference Inspector Herman's affidavit, Attachment C. [Doc. 28-2, p. 1.]

28. The search warrant was executed on March 28, 2002, and the following items, among others, were seized from Defendant's residence: 1 Gateway computer CPU [central processing unit], serial number 0015882168; eighty-eight 3½ inch floppy disks; and two writeable CDs. [Govt.'s Ex. 5.]

29. Robert Werbick has been a Postal Inspector since 1991. [Tr.-a.m. 49:16–17.]

30. Inspector Werbick specializes in computer forensic analysis. [Tr.-a.m. 49:18–25; 50:1, 21–23; 51:4–8.]

31. Inspector Herman sent the CPU, floppy disks, and CDs seized from Defendant's home to Inspector Werbick in Anaheim, California. [Tr.-a.m. 25:4–8.] Inspector Werbick conducted a search of all floppy disks. [Tr.-p.m. 15:3–25; 16:1–3.]

32. Inspector Herman also sent Inspector Werbick a cover letter requesting that he

examine the items and determine whether the information described in Attachment B existed within the files on the hard drive, the floppy disk or the CDs. [Govt's Ex. 2.]

33. Inspector Herman also sent Inspector Werbick a copy of the search warrant, which included Attachments A and B, and a copy of the search warrant application and affidavit. [Tr.-a.m. 25:11–19, 54:6–24; Govt's Ex. 5.]

34. Inspector Herman also sent Inspector Werbick a list that contained the names of known victims, their addresses, and credit card numbers that had been associated with fraudulent use [Govt's Ex. 6], and a list of the names and addresses of the residents on HCR 064. [Tr.-a.m. 25:11–19, 54:6–24; Govt's Ex. 6.]

35. Neither Government's Exhibit 6 (list of known victims) nor the list of the residents of HCR 064 were noted anywhere in Government's Exhibit 5.

36. Inspector Werbick crafted a key word search using the list of victim names provided by Inspector Herman. [Tr.-a.m. 59:2–18.]

37. Inspector Werbick did not employ a date restriction in his search of the computer. [Tr.-p.m. 21, 22:1–2.]

38. Inspector Werbick searched the entire computer hard drive for some of the victim names provided by Inspector Herman, without regard to when the file containing the data was created. [Transcript of afternoon proceedings ("Tr.-p.m.") 16:16–24.]

39. Inspector Werbick's key word search generated numerous "false hits," *i.e.*, a search term is located, but not in the form sought and not part of the items to be seized. [Tr.-a.m. 70:10–18; Tr.-p.m. 8:7–25, 9:1–14.]

40. Inspector Werbick's key word search generated several "positive hits," *i.e.*, an item that is within the scope of the items the search warrant authorized to be seized. [Tr.-a.m. 70:19–25.]

41. To determine whether a hit was false or positive, Inspector Werbick examined data surrounding the hit to determine whether it matched data he was requested to find. [Tr.-a.m. 71:3–19.]

42. Inspector Werbick found data on Defendant's computer containing the names of known victims of credit card fraud and the numbers of credit cards associated with fraudulent use. [Tr.-a.m. 71:20–25, 72:1–5; Govt's Ex. 7.]

43. Inspector Werbick also found on Defendant's computer a fragment of a spreadsheet-like document entitled "Credit Card Log" that listed account numbers, credit card company names, PIN numbers, and credit limits, with associated names and addresses. [Tr.-a.m. 72:8–13; Govt's Ex. 3.]

44. The location of the file fragment in unallocated space on the computer hard drive indicated to Inspector Werbick that there had been an attempt to delete the document identified as Government's Ex. 3. [Tr.-a.m. 73:10–16.]

45. Both Inspector Herman and Inspector Werbick "adopted" as true and accurate the factual recitations in the Government's written Response. [Tr.-a.m.

32:9–13; Tr.-p.m. 6:13–18.] For purposes of its factual findings, the Court declines to accept the wholesale adoption by Inspector Herman and Inspector Werbick of the Government's factual recitations set forth in its pleadings, and will consider only the sworn testimony of the witnesses at the hearing and other evidence specifically admitted.

46. I find that the testimony of Inspectors Herman and Werbick was credible.

II. LEGAL ANALYSIS

The Defendant seeks suppression of all evidence discovered as a result of the Government's search of her computer and computer disks on the grounds that the search warrant violated the Fourth Amendment's particularity requirement. The subject of the inquiry is the warrant's Attachment B.

A. Does the warrant lack particularity as to the computer search?

"The Fourth Amendment requires that a search warrant describe the things to be seized with sufficient particularity to prevent a general exploratory rummaging in a person's belongings." United States v. Carey, 172 F.3d 1268, 1272 (10th Cir. 1999) (citing Marron v. United States, 275 U.S. 192, 196 (1927)). A warrant that does not meet the particularity requirement does not pass constitutional muster, even if the application adequately describes the things to be seized. Groh v. Ramirez, 540 U.S. 551, 557 (2004).

The storage capacity of computers requires a special approach to the particularity requirement. Carey, 172 F.3d at 1275 n.7. Computers may contain a greater quantity and variety of information than any previous storage method, making them "tempting targets in

searches for incriminating information." Carey, 172 F.3d at 1275 (quotation marks and citation omitted). Because of the difficulties of conducting an on-site search of computers, the government frequently seeks and obtains authority to seize computers without any prior review of their contents. In re Search of: 3817 W. West End, First Floor Chicago, Ill 60621, 321 F.Supp.2d 953, 958 (N.D.Ill. 2004).

Seizing Defendant's computer and disks prior to reviewing their contents is what the Government obtained permission to do, and in fact, did in this case. Defendant does not claim that the Government should not have been allowed to seize the computer items or to conduct an off-site search of the seized computer items. She claims that the warrant failed to adequately identify the items that the Government could look for within the computer items it seized. Defendant argues that "the warrant did not restrict the government's search to matters relevant to [her] alleged criminal activity of embezzling mail from her postal route and using what she embezzled to commit credit card fraud." [Doc. 23 at 1.]

Attachment B describes four categories of "Computer Items to Be Seized." *See Finding of Fact No. 25, supra.* Inspector Herman testified that paragraph 6 was intended to allow seizure of software that would enable the computer analyst to access the computer and any files it contained; paragraph 7 was intended to allow seizure of items such as hard drives and external hard drives; paragraph 8 was intended to allow seizure of software that would enable the computer analyst to access the computer and any files it contained; and paragraph 9 was intended to allow seizure of printed materials concerning the operation of the computer. [Tr.-a.m. 23, 24:1–22.]

The descriptions of the computer items to be seized is undeniably comprehensive. Indeed, Inspector Herman testified that it was necessary to seize all the computer media and computer disks in Defendant's home because, although she believed evidence would be found on the computer, she was unsure where on the computer the evidence would be located. [Tr.-a.m. 24:23–25, 25:1–3.]

The Tenth Circuit has described one approach that law enforcement may use when conducting computer searches in cases where an on-site search is not feasible. Carey, 172 F.3d at 1275. If officers searching electronic media come across relevant documents so intermingled with irrelevant documents that they cannot feasibly be sorted at the site, they may hold the documents and seek approval from a magistrate of the conditions and limitations on a further search. Carey, 172 F.3d at 1275. "The magistrate should then require officers to specify in a warrant which type of files are sought." Carey, 172 F.3d at 1275. Although officers are not necessarily required to obtain second warrants before conducting a search of computer equipment that has been seized, they still "must be clear as to what it is they are seeking on the computer and conduct the search in a way that avoids searching files of types not specified in the warrant." United States v. Grimmett, 439 F.3d 1263, 1270 (10th Cir. 2006) (quotation marks and citation omitted).

The warrant at issue here purports to authorize the search and seizure of "any and all" computer items—without limitation. It is true that a computer search "may be as extensive as reasonably required to locate the items described in the warrant." Id. at 1270 (quoting United States v. Wuagneux, 683 F.2d 1343, 1352 (11th Cir. 1982)). However, the warrant

contains *no* restriction on the scope of the search the Government was authorized to conduct on Defendant's computer items, once they were seized. I thus conclude that the warrant is facially defective because it authorizes law enforcement to search all computer media seized from the Defendant's home, without telling them what to look for.

This omission does not constitute a mere technical mistake. With respect to the computer items, the warrant fails to identify the objects of the computer search. This is contrary to Tenth Circuit case law which "suggests that warrants for computer searches must affirmatively limit the search to evidence of specific federal crimes or specific types of material." United States v. Riccardi, 405 F.3d 852, 862 (10th Cir. 2005).

Furthermore, the Fourth Amendment "requires that the government describe the items to be seized with as much particularity as the government's knowledge allows, and warrants are conclusively invalidated by their substantial failure to specify as nearly as possible the distinguishing characteristics of the goods to be seized." Id. (quoting United States v. Leary, 846 F2d 592, 600 (10th Cir. 1988)). Information that could have more particularly described the items to be searched for on the computer was available, but omitted from both the warrant and the affidavit presented to the Magistrate Judge. Inspector Herman had the names and addresses of some known victims of credit card fraud before she applied for the warrant. She also presumably had or easily could have obtained a list of the customers on HCR 064.[1] However, none of this information was provided to the Magistrate Judge, listed

[1]It is noted that the search warrant was issued by Judge Deaton on March 27, 2002, and Inspector Herman's letter to Inspector Werbick is dated April 1, 2002, just five days later.

in the affidavit, or included in the warrant.

The Tenth Circuit cases begin with the premise that the warrant will identify particular files or information, so that officers can avoid searching files that are not identified in the warrant. See, e.g., Riccardi, 405 F.3d at 862 (holding that "officers conducting searches (and the magistrates issuing warrants for those searches) cannot simply conduct a sweeping, comprehensive search of a computer's hard drive."); Carey, 172 F.3d at 1276 (recognizing that "law enforcement officers can generally employ several methods to avoid searching files of the type not identified in the warrant: observing file types and titles listed on the directory, doing a key word search for relevant terms, or reading portions of each file stored in the memory"). The defect in the warrant in this case is that it does not identify *any* files or information. The entire hard drive, all the disks, and every byte of information were fair game for the search.

B. Do paragraphs 2, 3, and 5 of Attachment B limit the scope of the computer search?

The Government does not contend that it was entitled to conduct an unrestricted search of Defendant's computer items, or that it could have searched the computer items for evidence of crimes for which it did not have probable cause. It argues instead that the search of the computer items was limited by language contained in paragraphs 2, 3 and 5 of Attachment B. Both Inspector Herman and Inspector Werbick testified that they understood paragraphs 2, 3 and 5 as imposing limitations upon the search of the computer media seized from Defendant's home.

Paragraph 2 of Attachment B authorizes the Government to seize "[a]ny and all...records bearing names, addresses and/or credit card numbers of known victims and other residents from Highway Contract Route 064 in Los Lunas, New Mexico." Paragraph 3 authorizes the Government to seize "[a]ny and all...records related to credit card or other accounts at financial institutions and/or business for individuals other than residents of [Defendant's address.] Paragraph 5 authorizes the Government to seize "[a]ny and all...materials including...data and computer logs bearing victim information and/or other information related to or pertaining to the theft of mail, the fraudulent credit cards, bank fraud and conspiracy including but not limited to credit card offers, receipts, credit card statements, financial statements, and financial transaction records."

The Government's interpretation that paragraphs 2, 3, and 5 of Attachment B restrict the search of the computer items is not a reasonable construction of the warrant. Paragraphs 2, 3, and 5 are contained in a section titled "Items To Be Seized" that is separate from the "Computer Items To Be Seized" section below it. There is no reference in the "Computer Items To Be Seized" to the preceding "Items To Be Seized" section, and there is no language in the "Items To Be Seized" section indicating that it applies to "Computer Items To Be Seized." The implication of the two separately-titled sections is that the "Items To Be Seized" are *in addition* to the "Computer Items To Be Seized." The "Items To Be Seized" section thus broadens, rather than restricts the scope of the search.

The Court's conclusion that paragraphs 2, 3, and 5 do not restrict the search of the computer items is supported by the fact that Inspector Herman had to provide Inspector

Werbick information that was not contained in those paragraphs in order for him to craft the search criteria. Inspector Herman used the victim names and other information Inspector Herman sent him to construct the key word searches that revealed the victim information on the Defendant's computer and to distinguish false hits from positive ones.

The Government urges the Court not to invalidate the warrant based on a hypertechnical reading and cites United States v. Simpson for the proposition that courts should apply "a practical rather than a technical standard" to determine whether a warrant is adequate. The question in Simpson was whether a search of the defendant's property was beyond the scope of a warrant that authorized a search only of the defendant's "person." United States v. Simpson, 152 F.3d 1241, 1248 (10th Cir. 1998). Applying a practical rather than a technical standard, the Tenth Circuit held that the warrant sufficiently described the place to be searched as including defendant's residence. Simpson, 152 F.3d at 1248. By contrast, the warrant here was both practically *and* technically insufficient. From a practical perspective, Inspector Werbick could not have conducted the search that he did without supplemental information from Inspector Herman. Paragraphs 2, 3, and 5 provided no particularized guidance regarding what Inspector Werbick was to search for in terms of victim information. In other words, there is nothing in these paragraphs either to facilitate or to restrict the computer search.

I conclude, therefore, that paragraphs 2, 3, and 5 of Attachment B do not limit the scope of the computer search. The warrant is overbroad and thus fails to satisfy the Fourth Amendment's particularity requirement.

Inspector Herman's affidavit in support of the warrant application (Attachment C) does not save the overbroad warrant. An affidavit can be considered in assessing particularity only if it is attached to the warrant *and* incorporated by reference. Riccardi, 405 F.3d at 863 n.1; see also United States v. Williamson, 1 F.3d 1134, 1136 n.1 (10th Cir. 1993) (stating that affidavit can cure defective warrant only when affidavit is physically connected to, and referenced by warrant). Our Circuit has stated that an affidavit can cure an overbroad warrant only when two requirements are satisfied. First, "the affidavit and search warrant must be physically connected so that they constitute one document; and second, the search warrant must expressly refer to the affidavit and incorporate it by reference using suitable words of reference." Leary, 846 F.2d at 603 (citations and quotation marks omitted). I have previously found that the affidavit, denominated "Attachment C," was attached to the warrant. Thus, the first prong is satisfied. However, the warrant did not expressly incorporate the affidavit; there is no specific reference to the affidavit on the face of the warrant (unlike the warrant's express reference and incorporation of Attachments A and B). The second prong, therefore, is not satisfied and the affidavit is not subject to consideration for curing the defects in the overbroad warrant. I further note in this regard that even if the technical requirements for incorporation by reference had been satisfied in this case, the affidavit does not supply the necessary particularity (such as names and addresses of mail route customers and suspected victims, which information was known to Inspector Herman prior to the preparation of the affidavit) to cure the deficiency in the warrant.

C. Does the "good faith" exception apply?

The Government submits that if the warrant lacked particularity and such defect could not be cured by reference to the affidavit, the evidence obtained from the computer hard drive should not be suppressed because the postal inspectors acted in good faith in executing the warrant.

It is well established that evidence seized pursuant to an invalid warrant does not necessarily have to be suppressed. In United States vs. Leon, 468 U.S. 897 (1984), our Supreme Court recognized an exception to the exclusionary rule when officers acted in good faith and in reasonable reliance on an invalid warrant in executing their search. See also Riccardi, 405 F.3d at 863 (citing Leon, 468 U.S. 897); United States vs. Gonzales, 399 F.3d 1225, 1229 (10th Cir. 2005). The good faith exception recognizes that the purposes of the exclusionary rule are not served by suppressing the fruits of a search conducted pursuant to a warrant issued in error by a neutral and detached judge where the law enforcement officer who obtains and executes the warrant has done so in good faith. "Penalizing the officer for the magistrate [judge's] error, rather than his own, cannot logically contribute to the deterrence of Fourth Amendment violations." Leon, 468 U.S. at 921. "The good faith exception does not apply, however, when the warrant is so facially deficient that it fails to "particularize the place to be searched or the things to be seized." United States v. Corral-Corral, 899 F.2d 927, 933 (10th Cir. 1990). The Government bears the burden of showing that the good faith exception applies. Corral-Corral, 899 F.2d at 932.

In determining whether the good faith exception should apply in a particular case, the Court's inquiry is confined "to the objectively ascertainable question whether a reasonably

well-trained officer would have known that the search was illegal despite the magistrate's authorization." Riccardi, 405 F.3d at 863 (citing Leon, 468 U.S. at 922 n.23). "In answering this question, the court should consider all of the circumstances and assume that the executing officers have a 'reasonable knowledge of what the law prohibits.'" Id. (quoting Leon, 468 U.S. at 919 n.20) (quotation marks in original).

As our Circuit recently noted, "[W]hile officers are generally entitled to rely on the magistrate's judgment, they are also required to exercise their own professional judgement. Indeed, law enforcement officials are presumed to have a reasonable knowledge of the law... and we determine good faith in this context by considering whether a 'reasonably well trained officer would have known that the search was illegal despite the magistrate's authorization.'" Gonzales, 399 F.3d at 1230 (quoting and citing Leon, 468 U.S. at 919 n.20, 922 n.23) (citation omitted).

In this case, where I have found that the warrant is facially invalid, I must also review the text of the warrant together with the circumstances of the search of the computer's hard drive to ascertain whether the agents might have reasonably presumed it to be valid. Riccardi, 405 F.3d at 863.

After conducting such a review, I conclude that the Government has not met its burden of showing that the good faith exception applies in this case. The warrant, including its Attachments A and B, is devoid of any limitation on the computer search, notwithstanding the Postal Inspector Werbick's subjective belief to the contrary. As stated previously, the search was only possible because Inspector Herman provided to the searcher, Inspector

Werbick, separate lists of victim names and HCR customers, which lists were external to the face of the warrant and not included in Attachments A, B or C. Such lists contained specific information as to identities of potential victims and as to all persons residing along Defendant's mail route, and none of this information was mentioned in the warrant and accompanying documentation (Ex. 1). These extrinsic lists served to fill-in large information gaps in the deficient warrant in a circumstance where much, if not all of this information, was know to Inspector Herman prior to her preparation of the warrant. Inspector Werbick did not participate in the investigation or in the preparation of the affidavit, and thus did not possess the knowledge that one actively involved in the investigation had.

In reviewing the text of the warrant and the circumstances of the search of the hard drive, which circumstances included the application of extrinsic specific information not mentioned in the warrant, I conclude that the warrant offered no guidelines as to the objects of the computer search and that the officer executing the search (Werbick) was given complete discretion in determining not only the manner of search, but also the objects of the search. As noted above, Inspector Werbick, was not involved in the investigation nor did he participate in preparing the application or affidavit. He therefore could not have independently conducted a limited search based on his own previous knowledge of the case. Compare Gonzales, 399 F.3d at 1230 (reasoning that when the underlying documents are devoid of factual support, an officer cannot be said to rely on them in good faith), with Riccardi, 405 F.3d at 864 (concluding that good faith exception applied because, among other reasons, officers executing warrant were involved in investigation). Absent limitations

in the warrant, Inspector Werbick was free to conduct, and did conduct, a free-ranging search of the computer items.

And even if Inspector Werbick exercised restraint, his restraint in this case is not a substitute for restraint imposed by a judicial officer through a proper warrant. See Groh, 540 U.S. at 561 (citing Katz v. United States, 389 U.S. 347 (1967)). The supplemental information provided to him by Inspector Herman might have aided his search, but it did not constitute a legal restriction on his authority. Furthermore, it appears that the search was not performed in a particularly limited manner. The search methodology was not confined in scope to items for which the Government had probable cause to search. Specifically, Inspector Herman did not include a date limitation in her request to Inspector Werbick. Inspector Herman's affidavit states that Defendant had been the contractor for HCR 064 for approximately 13 years. Reports of credit card fraud on HCR 064, however, did not begin until February 2001. As part of her investigation, Inspector Herman sought information from residents of HCR 064 regarding credit card fraud for the two years preceding March 2002. However, Inspector Herman did not request and Inspector Werbick did not employ a similar date restriction when he searched Defendant's computer. Numerous false hits were obtained with the victim name key word search. To distinguish a false hit from a positive one, Inspector Werbick had to examine data in proximity to the hits, which required him to view non-relevant personal information that was outside the scope of the warrant. Though there is no evidence that a date restriction would have reduced the number of false hits, it is logical to assume that adding a date restriction to a key word search would have resulted in a less

intrusive search.

D. The "Fruit of the Poisonous Tree" Doctrine

Finally, I address the scope of the evidence that must be suppressed as a result of the lack of particularity in the portions of the search warrant pertaining to the computer items. "A party seeking exclusion of evidence on Fourth Amendment grounds must demonstrate both actual police misconduct that violated the defendant's Fourth Amendment rights, and that the evidence to be excluded was in fact a product of the police misconduct." United States v. Williams, 356 F.3d 1268, 1272 (10th Cir. 2004) (citing United States v. DeLuca, 269 F.3d 1128, 1132 (10th Cir. 2001) and United States v. Nava-Ramirez, 210 F.3d 1128, 1131 (10th Cir. 2000)). "'Only if the defendant has made these two showings must the government prove that the evidence sought to be suppressed is not "fruit of the poisonous tree," either by demonstrating the evidence would have been inevitably discovered, was discovered through independent means, or was so attenuated from the illegality as to dissipate the taint of the unlawful conduct.'" DeLuca, 269 F.3d at 1132 (quoting Nava-Ramirez, 210 F.3d at 1131) (citations omitted). "It is thus incumbent upon a defendant to demonstrate some affirmative link between the police misconduct and the evidence obtained." Williams, 356 F.3d at 1272.

In this case, Defendant has demonstrated an affirmative link between the lack of particularity in the search warrant and the electronic data, files, or documents located on the hard drive that was seized during the warrant's execution. The Government has not asserted, much less proven, that any such information on the hard drive would have been found

through other means that were untainted by the lack of particularity in the search warrant. Thus, all electronic data, files, or documents found on the hard drive must be suppressed under the exclusionary rule.

On the other hand, Defendant has not asserted, much less proven, that there is any evidence extrinsic to the computer hard drive which would not have come to light but for the Government's unconstitutional search of the data on that hard drive. Accordingly, the scope of the exclusionary rule's application in this case is limited to the hard-drive data itself.

III. CONCLUSION

In light of the foregoing, I conclude that the warrant in the present case is so facially deficient that it could not reasonably be presumed valid for purposes of the Leon good faith exception. The Court will grant Defendant's motion to suppress all evidence seized as a result of the search of the computer hard drive and disks (i.e., the data on or retrieved from the computer hard drive and disks).

IT IS, THEREFORE, ORDERED that *Defendant's Motion to Suppress Evidence Seized from Her Computer and Computer Disks* [Doc. 23] filed December 11, 2007 is **GRANTED**.

SO ORDERED this 6th day of June 2008**,** in Albuquerque, New Mexico.

M. CHRISTINA ARMIJO
United States District Judge